



دليل الوقاية من عمليات الاحتيال المالي

البنك المركزي السعودي
SAMA
Saudi Central Bank





أساليب الاحتيال المالي تتجدد بشكل مستمر، وتتطور بتطور التقنية وظهور خدمات ومنتجات مالية جديدة.

يستخدم المحتالون أساليب متعددة لإيقاع الأفراد في عمليات الاحتيال؛ منها أساليب نفسية مثل الترهيب والترغيب، أو تقنية مثل الاختراق أو الروابط التصيدية أو إنشاء مواقع وتطبيقات إلكترونية مزيفة.

إن خط الدفاع الأول أمام عمليات الاحتيال المالي هو أنت.

لا تفرط ببياناتك الشخصية والمالية لأي جهة كانت وثبت دائماً من مصداقية ونظامية أي جهة تطلب هذه البيانات.



لماذا قد أتعرض إلى عملية احتيال مالي؟

- إفشاء معلوماتك المالية والشخصية لأشخاص وجهات مجهولة
- تمكين الآخرين من استخدام بطاقتك المصرفية وإجراء عمليات الدفع بها أو السماح بإجراء عملية الدفع عند أجهزة نقطة البيع بعيدًا عنك.
- التهاون في فتح الروابط الإلكترونية المجهولة التي تصل عبر البريد الإلكتروني أو وسائل التواصل الاجتماعي.
- استخدام مواقع إلكترونية غير موثوقة للتسوق وإدخال البيانات المالية لإجراء عمليات الدفع في هذه المواقع.
- الاستعجال في تقديم المعلومات المالية والشخصية دون التثبت من الجهة التي يتم التعامل معها.

يجب أن تعرف... أبرز أساليب الاحتيال المالي

- يستغل ممارسو الاحتيال الحاجات النفسية للأفراد لإيقاعهم في عمليات الاحتيال؛ مثل رغبتهم في الثراء السريع أو الفوز بجائزة مالية أو عينية أو الحصول على وظيفة أو تمويل.
- يستخدم ممارسو الاحتيال أساليب نفسية مثل استعجال الأفراد بتقديم معلوماتهم الشخصية والمالية لمنعهم من التريث والتفكير بالموقف وتقييم خطورته، أو ترهيبهم بادعاء أن حساباتهم البنكية سيتم تجميدها، أو ترغيبهم عن طريق تقديم حسومات أو جوائز.
- يستغل ممارسو الاحتيال عدم معرفة الأفراد بالجهات المالية المرخصة أو الإجراءات الرسمية للحصول على الخدمات والمنتجات المالية.
- ينتحل ممارسو الاحتيال صفة جهات حكومية أو مالية أو تجارية معروفة من خلال استخدام أسماء وشعارات تلك الجهات وإنشاء مواقع إلكترونية مزيفة وإرسال روابط إلكترونية بعناوين مشابهة لعناوين تلك الجهات بحيث يصعب اكتشاف الفرق بينها.

نصيحة: لا تفتح أي رابط يصلك عبر البريد الإلكتروني مهما بدا مقنعًا،
وافتح الموقع الإلكتروني الذي تريد من خلال المتصفح.

كيف أتجنب عمليات الاحتيال المالي؟

في عمليات الاحتيال المالي، أنت خط الدفاع الأول.

لتحمي نفسك من عمليات الاحتيال، اتبع الخطوات الأربع الآتية:

إعرف

كن على معرفة واطلاع مستمر بأساليب الاحتيال المالي والتحذيرات التي تنشرها الجهات الحكومية المعنية.

تمهل

لا تتسرع في تقديم بياناتك الشخصية والمالية لأي جهة كانت سواءً عبر رابط إلكتروني، أو رسالة نصية، أو موقع إلكتروني، أو مكالمة هاتفية تدعي أنها من جهة حكومية أو تجارية.

تثبت

تأكد من هوية ونظامية أي جهة تطلب بياناتك الشخصية والمالية بطريقة غير رسمية عبر الرسائل النصية، أو الروابط البريدية، أو وسائل التواصل الاجتماعي فهي في الغالب عملية احتيال.

بلغ

بلغ الجهة المالية التي تتعامل معها والجهات الأمنية المختصة على الفور في حال اشتبهت أنك تعرضت إلى عملية احتيال مالي.

إرشادات عامة

- حافظ على سرية معلوماتك الشخصية ومعلومات بطاقتك المصرفية ولا تفشها لأي شخص أو جهة كانت.
- استخدم المواقع والتطبيقات الإلكترونية الرسمية للجهات المالية لإجراء العمليات المالية، وحملها من مصادر رسمية وموثوقة.
- افتح المواقع الإلكترونية الرسمية من عناوينها الرسمية فقط؛ ولا تضغط على أي رابط يصلك يدعي أنه جهة تجارية أو حكومية أو مالية.
- لا تعط بطاقتك المصرفية لأي شخص لإجراء عملية الدفع، وتأكد أن يتم إجراء العملية أمامك.
- عند فقدان بطاقة الصرف الآلي أو البطاقة الائتمانية، سارع بالاتصال بالبنك المصدر للبطاقة للإبلاغ عن فقدانها، وإيقافها فوراً.
- ضع يدك على لوحة الأرقام في جهاز الصرف الآلي أو نقاط البيع عند إدخال الرقم السري.
- غير الرقم السري لجميع بطاقات الصرف الآلي والبطاقات الائتمانية بشكلٍ دوري وبعد العودة من السفر خارج المملكة عبر قنوات التواصل الرسمية من البنك.
- لا تستجب لطلبات المساعدة من مجهولين أثناء استخدام جهاز الصراف الآلي أو سداد الفواتير.
- ثبت برامج حماية على جوالك أو حاسوبك الشخصي لجعل تصفح الإنترنت أكثر أماناً.
- أبلغ البنك فوراً عن أي معاملات مشبوهة على البطاقة المصرفية لإيقافها واتخاذ الإجراءات اللازمة لحماية العملاء الآخرين.
- لا تستخدم رقم سري واحد لأكثر من بطاقة مصرفية.
- لا تشارك رمز التحقق المرسل إلى جوالك من الجهة المالية مع أي طرف آخر حتى لا تُعرض حساباتك البنكية وأموالك إلى السرقة.



الشراء الآمن عبر الإنترنت

أصبح الدفع الإلكتروني عبر الإنترنت جزءاً أساسياً من تعاملاتنا الرقمية لسهولة وسرعته وأمانه.

تساهم الإرشادات الآتية في تعزيز أمان عمليات الدفع الإلكتروني :

- تجنب تفعيل خاصية الشراء عبر الإنترنت للبطاقة المصرفية في حال عدم استخدامك لهذه الخاصية.
- تأكد من موثوقية وأمان الموقع أو التطبيق الخاص بالمتجر الإلكتروني عند الشراء عبر الانترنت.
- تأكد من موثوقية شبكة الاتصال اللاسلكية (Wi-Fi) عند التسوق عبر الإنترنت.
- تحقق من كشف الحساب البنكي والرسائل النصية الواردة من البنك للتأكد من عدم تنفيذ أي عمليات مالية غير مفوضة منك.
- لا تحفظ بيانات البطاقة المصرفية في مواقع وتطبيقات التسوق الإلكترونية غير الموثوقة.
- حافظ على سرية معلومات البطاقة المصرفية ولا تشارك هذه المعلومات مع آخرين لتنفيذ عمليات الشراء عبر الإنترنت.



ماذا أفعل إذا تعرضت لعملية احتيال مالي؟

أبلغ الجهة المالية التي تتعامل معها والجهات الأمنية المختصة على الفور في حال اشتبهت أنك تعرضت إلى عملية احتيال مالي.

كيف أتصرف إذا وصلتني رسالة احتيال؟

أعد إرسال الرسالة النصية الواردة إليك مع رقم المرسل إلى الرقم الموحد: **330330**

خط الدفاع الأول لتجنب عمليات الاحتيال المالي
هو أنت.

.....

تذكر..

الخطوات الأربع للوقاية من الاحتيال المالي:
اعرف، تمهل، تثبت، بلِّغ

WWW.SAMA.GOV.SA

 WWW.SAMACARES.SA
 @SAMAcareS

